Remarks

Claims 1, 3 and 6-13 are pending in the present application. Reconsideration and allowance are requested in view of the above amendments and the remarks below.

Claims 1-14 are rejected under 35 U.S.C. 103(a) over Jobst et al. (U.S. Patent No. 6,707,915), hereafter "Jobst," in view of Koukoulidis et al. (U.S. Patent Publication No. 2003/0123669), hereafter "Koukoulidis." This rejection is defective because the combination of Jobst and Koukoulidis fails to teach or suggest each and every feature of the claims as required by 35 U.S.C. 103(a).

To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations.

In this case, the rejection is defective because, *inter alia*, the references of Jobst and Koukoulidis, taken alone or in combination, fail to teach or suggest each and every feature of the claims as required by 35 U.S.C. 103(a).

Claim 1 sets forth:

"A text messaging system for the encryption of a text message sent to a wireless terminal equipment, the text message comprising a Short Message Service (SMS) message having a User Data Header (UDH) and a text data field, the text messaging system comprising:

means for storing an equipment identification number uniquely assigned to the wireless terminal equipment, wherein the assigned equipment identification number is an International Mobile Equipment Identity (IMEI) number of the wireless terminal equipment;

means coupled to the equipment identification number storing means for encrypting the text data field content of the SMS message using only the IMEI number assigned to the wireless terminal equipment as the shared key; and

means for setting an encryption identifier in an Information Element (IE) group of the UDH of the SMS message, the encryption identifier comprising a marker in an IE data field, the IE group further comprising an Information Element Identifier (IEI) field set to indicate a presence of the marker, and an Information Element Data Length (IEDL) field set to indicate a length of the marker."

Jobst does not disclose, *inter alia*, the claimed "means coupled to the equipment identification number storing means for encrypting the text data field content of the SMS message using only the IMEI number assigned to the wireless terminal equipment as the shared key." On the contrary, Jobst discloses in column 2, lines 38-42, that the "phone password is stored in the phone and is calculated by **combining** the IMEI number and the Master Password by means of a secure hash algorithm, such as a public key algorithm (for example, the MD5 algorithm from the RSA Data Security Company." However, nowhere does Jobst disclose that **only the IMEI number is used as a shared key** for the encryption of the text data field content. Rather, Jobst discloses that the **combination** of the IMEI number and the Master Password is encrypted using an **undisclosed public/shared key**.

Koukoulidis does not remedy the glaring deficiencies of Jobst. Further, Koukoulidis, which the Examiner has relied on as disclosing encryption/decryption of SMS messages, does not disclose, *inter alia*, the claimed "means for setting an encryption identifier in an Information Element (IE) group of the UDH of the SMS message, the encryption identifier comprising a marker in an IE data field, the IE group further comprising an Information Element Identifier (IEI) field set to indicate a presence of the marker, and an Information Element Data Length (IEDL) field set to indicate a length of the marker." Rather, Koukoulidis discloses the use of a complex and convoluted, multi-SMS message protocol for secure transactions. For example, Koukoulidis discloses (Abstract):

"The center encrypts an authorization key in response to a wireless terminal's SMS message containing a public key and a request for the authorization key, sends back to the wireless terminal an SMS message containing the encrypted authorization key, decrypts another SMS message received from the wireless terminal which contains an authentication code and a request for a traffic key, authenticates the SMS message, encrypts the traffic key, and sends to the wireless terminal another SMS message containing the traffic key."

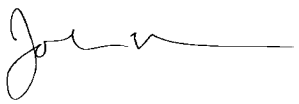
Unlike Koukoulidis, the present invention takes advantage of a free Information Element (IE) group in the a User Data Header (UDH) of an SMS message to provide for the encryption/decryption of the text data field of the SMS message.

Accordingly, since Jobst and Koukoulidis, taken alone or in combination, fail to teach or suggest each and every feature of independent claim 1 as required by 35 U.S.C. 103(a), Applicants respectfully submit that independent claim 1 and its

corresponding dependent claims 3 and 6-10 are allowable. Applicants further submit that independent claim 11 and its corresponding dependent claims 11-13 are allowable for reasons similar to those set forth above with regard to independent claim 1.

If the Examiner believes that anything further is necessary to place the application in condition for allowance, the Examiner is requested to contact Applicants' undersigned representative at the telephone number listed below.

Respectfully submitted,



Dated: September 28, 2006

John A. Merecki
Reg. No. 35,812

Hoffman, Warnick & D'Alessandro LLC
75 State Street, 14th Floor
Albany, NY 12207
(518) 449-0044 - Telephone
(518) 449-0047 - Facsimile